What is Claimed is:

1. A method comprising:

receiving network data;

reassembling a client-server communications session from the network data; and

detecting, through the network data, leaks of information by analyzing the client-server communications session using at least one of (i) statistical and (ii) keyword - based detection.

2. The method of claim 1, further comprising

decoding the client-server communications session to detect and inspect one or more application protocols, and

wherein the client-server communications session includes the one or more application protocols.

3. The method of claim 2, wherein the one or more application protocols includes at least one of (i) pdf, (ii) http, (iii) e-mail, (iv) e-mail attachment, (v) ftp, (vi) zip, (vii) ms word, (viii) ms excel, (ix) html, (x) xml, (xi) gzip, (xii) tar and (xiii) plain text.

4. The method of claim 1, wherein the client-server communications session includes at least one of (i) TCP, (ii) IP and (iii) ethernet.

5. The method of claim 1, wherein the statistical-based detection includes multi-dimensional content profiling.

6. The method of claim 1, wherein the statistical-based detection includes domain-specific high-level features.

7. The method of claim 6, wherein the domain-specific high-level features includes at least one of (i) social security numbers, (ii) credit card numbers, (iii) postal addresses and (iv) e-mail addresses.

8. The method of claim 1, wherein the keyword-based detection includes one or more weighted keywords.

9. The method of claim 1, wherein the information includes a digital asset.

10. The method of claim 1, further including

analyzing the network data so as to detect any unauthorized encrypted session.

11. A method comprising:

receiving network communications; and

preventing an unauthorized and/or malicious transfer, through the network communications, of data by providing at least content reassembly, scanning and recognition to the network communications in real time.

12. The method of claim 11, wherein the content scanning and recognition includes multi-dimensional content profiling.

13. The method of claim 11, wherein the content scanning and recognition is tailored to local data.

14. The method of claim 11, wherein the method is capable of preventing the unauthorized and/or malicious transfer, through the network communications, of data on fully saturated Gigabit speeds.

15. A method comprising:

receiving network data; and

preventing, through the network data, leaks of information by at least applying multi-dimensional content profiling.

16. The method of claim 15, wherein the information includes a digital asset.

17. The method of claim 15, wherein the multi-dimensional content profiling takes into account the structure of the information.

18. A machine-readable medium having encoded information, which when read and executed by a machine causes a method comprising:

receiving network data;

reassembling a client-server communications session from the network data; and

detecting, through the network data, leaks of information by analyzing the client-server communications session using at least one of (i) statistical and (ii) keyword - based detection.

19. A machine-readable medium having encoded information, which when read and executed by a machine causes a method comprising:

receiving network communications; and

preventing an unauthorized and/or malicious transfer, through the network communications, of data by providing at least content reassembly, scanning and recognition to the network communications in real time.

20. A machine-readable medium having encoded information, which when read and executed by a machine causes a method comprising:

receiving network data; and

preventing, through the network data, leaks of information by at least applying multi-dimensional content profiling.

21. An apparatus comprising:

a receiver to receive network data;

a processor, coupled to the receiver, to (i) reassemble a client-server communications session from the network data and (ii) detect, through the network data, leaks of information by analyzing the client-server communications session using at least one of (i) statistical and (ii) keyword -based detection.

22. An apparatus comprising:

a receiver to receive network communications; and

a processor, coupled to the receiver, to prevent an unauthorized and/or malicious transfer, through the network communications, of data by providing at least content reassembly, scanning and recognition to the network communications in real time.

23. An apparatus comprising:

a receiver to receive network data; and

a processor, coupled to the receiver, to prevent, through the network data, leaks of information by at least applying multi-dimensional content profiling.